in-depth expert Knowledge

70+ white-hat hackers

50+ certifications

vulnerability lab

numerous **publications**

long-lasting Experience

10+ years consulting

400+ projects per year

bsi. ISO/IEC 27001 Information Security Management

full range of Services

Resilience Framework

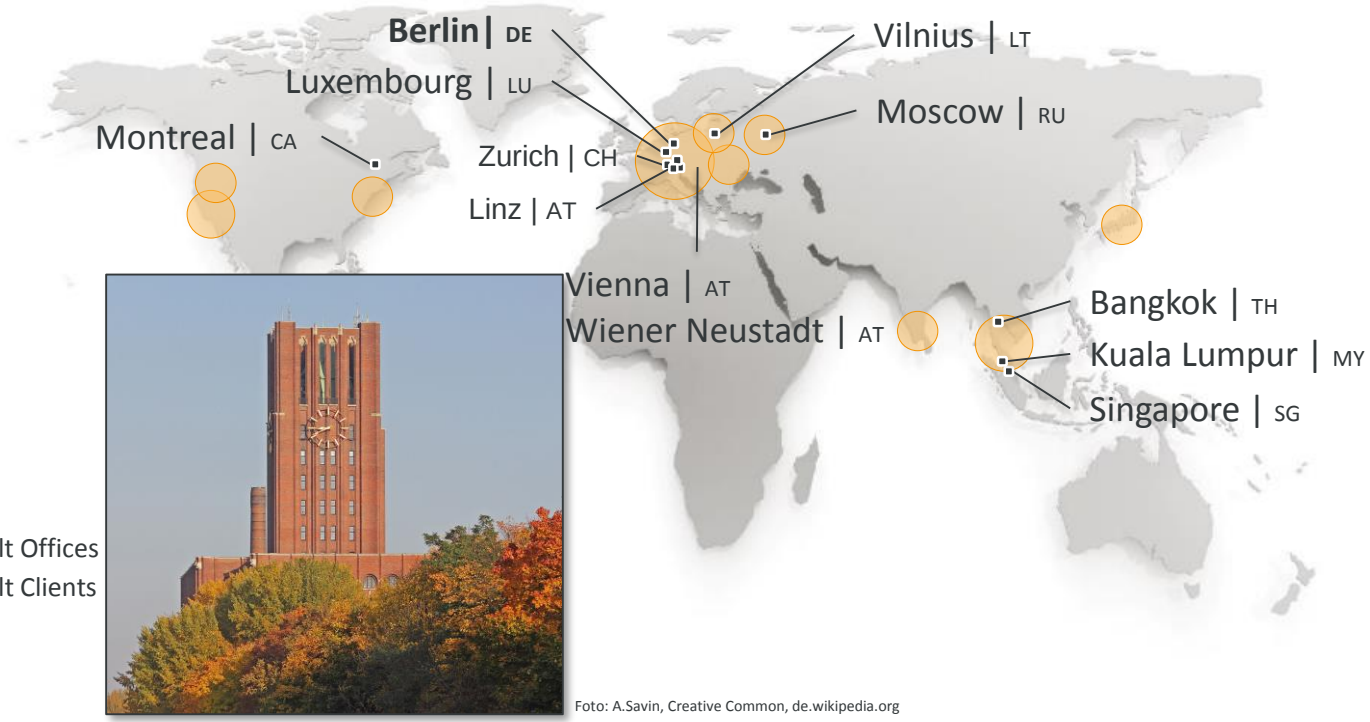


Foto: A.Savin, Creative Common, de.wikipedia.org

Internet of Things.
what is it exactly?

The Internet of Things (IoT) is the network of dedicated physical objects (things) that contain embedded technology to **sense or interact** with their internal state or external environment.

The IoT comprises an **ecosystem** that includes things, communications, applications and data analysis.

Source: Gartner, The Internet of Things and Related Definitions, 23.10.2014

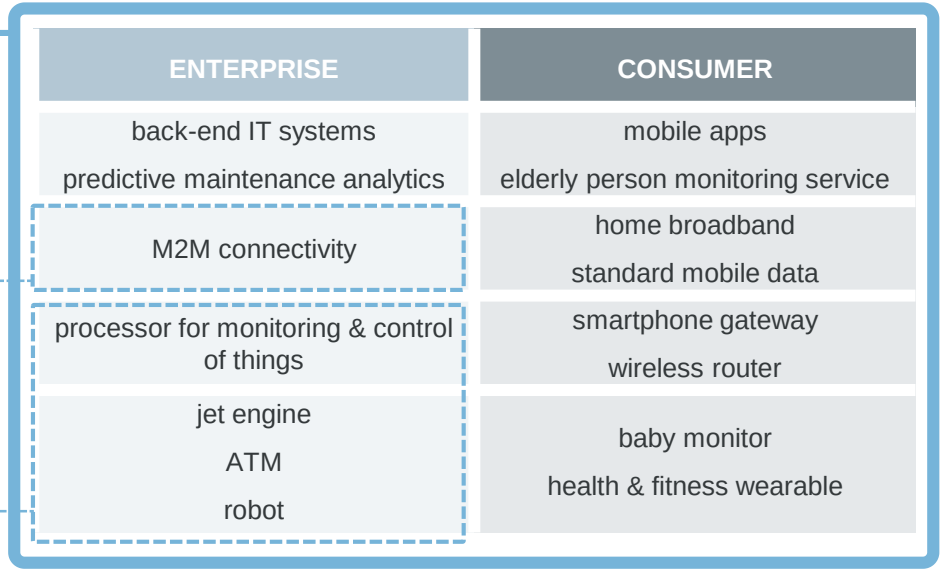
Example Enterprise vs. Consumer IoT

Internet of Things

M2M Communication Services

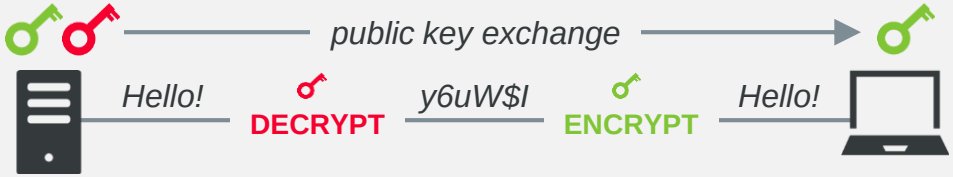
Operational Technology

(can include stand alone machines outside of the IoT)



Source: Gartner, The Internet of Things and Related Definitions, 23.10.2014

Asymmetric Encryption Basics



Server generates key pair (e.g. RSA public and private key)

Server keeps private key private!

Server provides public key to clients

Clients can encrypt information with the public key for the server

Server can decrypt information with the private key

Client and server establish secure channel

SSH and HTTPS

SSH – Secure Shell

- cryptographic network protocol
- for operating network services securely over an unsecured network

HTTPS – Hypertext Transfer Protocol Secure

- protocol for secure communication over a computer network

Security for the Internet of Things

The Internet of Things is an **increasingly attractive early link in attack chains**. IoT vendors remain likely to **repeat the security mistakes of the past** and not embrace modern security, vulnerability management and disclosure practices. […]

Source: Gartner, Predicts 2016: Security for the Internet of Things, 9.12.2015

how **risky** is the **key handling** in firmware of IoT (embedded) devices in general?

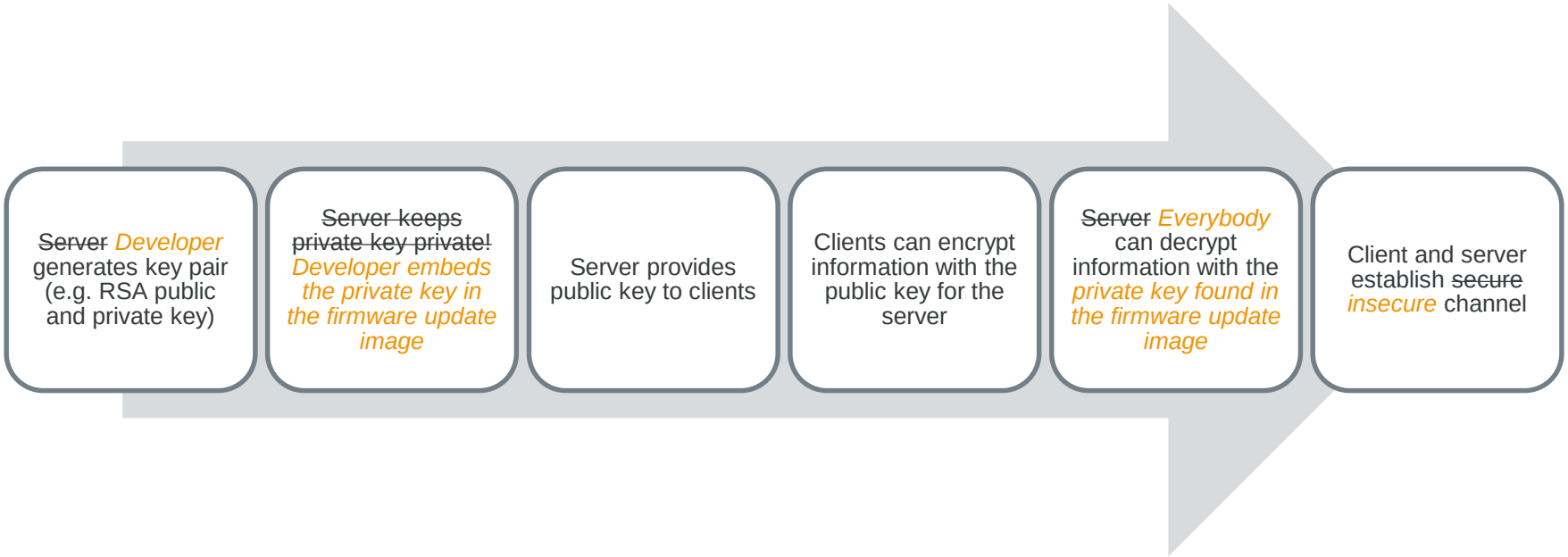
We did a large scale security analysis to find out.

4000 devices

70 vendors

internet gateways, routers, modems, IP cameras, VoIP phones, M2M, etc.

Finding #1 – **Incorrect Asymmetric Encryption Basics**



Finding #2 – **Wrong Configuration & Exposure to the Internet**

9% of all HTTPS
hosts on the web use
hardcoded certificates

3.2 million HTTPS hosts
on the web use
~150 unique key pairs

6% of all SSH
hosts on the web use
hardcoded certificates

0.9 million SSH hosts
on the web use
~80 unique key pairs

What are the impacts of those vulnerabilities?

The private keys are known so the following attacks are possible:

- impersonation of servers
- man-in-the-middle attacks
- passive decryption attacks

Attack vectors:

- from local network easily feasible
- “global adversary” scans internet traffic

Why are so many devices exposed to the web?

Insecure default configuration by vendor

- Services exposed on WAN interface
- Automatic port forwarding using UPnP

Insecure configuration by purchaser

- ISP configuration of CPE devices

Top 10 Countries

(% of all affected hosts based on IP addresses, HTTPS / SSH)

1	United States	**26,27%**
2	Mexico	**16,52%**
3	Brazil	**8,10%**
4	Spain	**5,60%**
5	Colombia	**4,36%**
6	Canada	**3,25%**
7	China	**3,20%**
8	Russian Federation	**2,36%**
9	Taiwan	**2,27%**
10	United Kingdom	**2,26%**

Why are so many devices exposed to the web?

ISPs with a particularly bad track record:

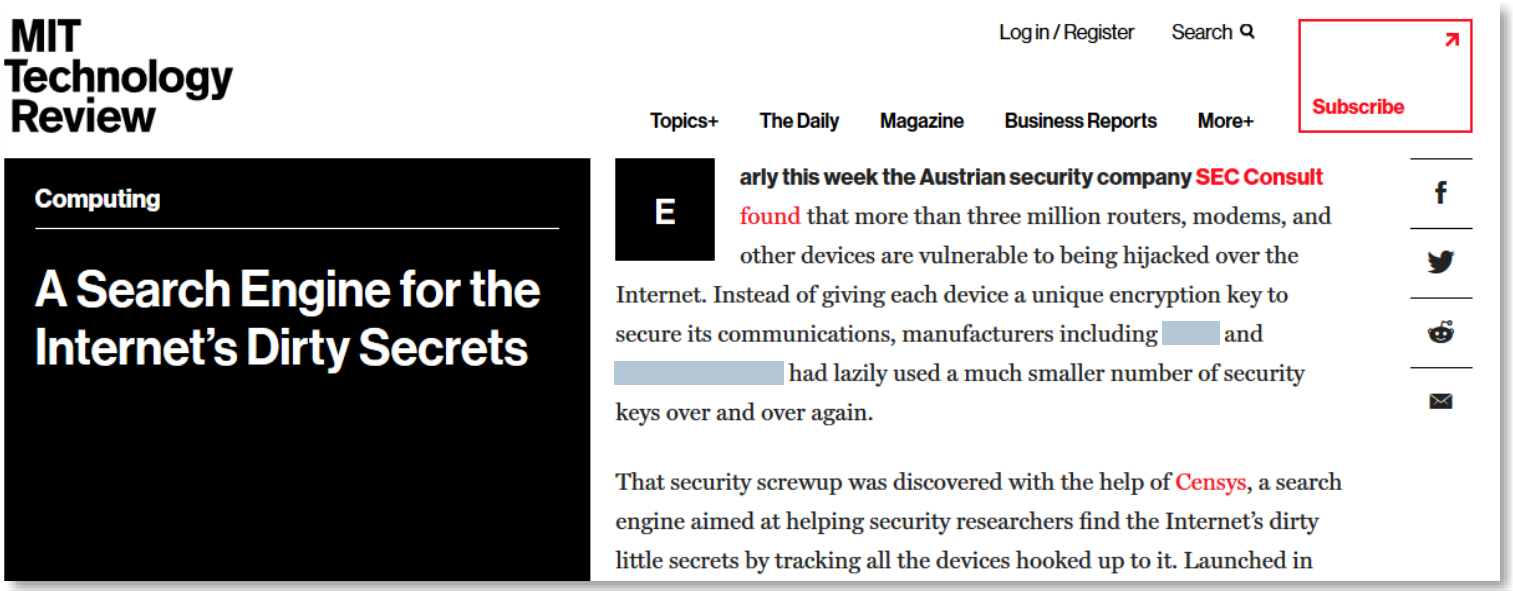
- **Mexican Telco** exposes HTTPS remote administration on **more than 1,000,000** of their subscribers devices
- **US-based ISP** exposes HTTPS remote administration on **more than 500,000** devices
- **Telco in Spain** exposes SSH remote administration on **more than 170,000** devices
- **Chinese Teleco** exposes SSH remote administration on **more than 100,000** devices

Read the full story on blog.sec-consult.com.

Affected vendors (excerpt)

Censys

IoT search engine used to correlate results:



MIT Technology Review

Log in / Register Search

Topics+ The Daily Magazine Business Reports More+

Subscribe

Computing

A Search Engine for the Internet's Dirty Secrets

Early this week the Austrian security company SEC Consult found that more than three million routers, modems, and other devices are vulnerable to being hijacked over the Internet. Instead of giving each device a unique encryption key to secure its communications, manufacturers including [redacted] and [redacted] had lazily used a much smaller number of security keys over and over again.

That security screwup was discovered with the help of Censys, a search engine aimed at helping security researchers find the Internet's dirty little secrets by tracking all the devices hooked up to it. Launched in

Source: www.technologyreview.com/s/544191/a-search-engine-for-the-internets-dirty-secrets/

more than 900 products from 50 vendors are affected.

informing all vendors is a mammoth task…

Affected Products – Coordination

SEC Consult teamed up with CERT/CC

(Carnegie Mellon University) to contact all affected vendors

(CERT Vulnerability Note VU#566724)

a few responded

fewer made fixes available

even fewer devices get actually implemented fixes

More detailed information on www.sec-consult.com and blog.sec-consult.com

Official CERT Vulnerability Note & affected Vendors

Vendor Information for VU#566724

Embedded devices use non-unique X.509 certificates and SSH host keys

https://www.kb.cert.org/vuls/id/566724

Down the **IoT supply chain**

Authentication bypass and OEM backdoors in WiMAX routers

Authentication bypass:

- Attacker can change the any settings without authentication via Web-UI
- Includes admin password

Backdoor accounts:

- Attacker can login via Telnet/SSH
- Mirai botnet exploited same vulnerability class

more than 80,000 devices are exposed on the web

Read the full story on blog.sec-consult.com.

Attribution

Who is affected?

IoT Inspector plugin

- WiMAX Routers by **ZyXEL**
- WiMAX Routers by **MitraStar** (ZyXEL's sister company)
- WiMAX Routers with OEM **ZyXEL/MitraStar**
    - with **Huawei** branding
    - with **ZTE** branding
    - with **GreenPacket** branding

All products have same code base for the firmware

```
#!/bin/sh
#
# @author bohao.lin@zyxel.com.tw
#
#

# 2010-1028 bohao.lin@zyxel.com.tw
# SYNC sncfg's account (ADMIN_NAME and GUEST_NAME) to Linux shadow/passwd.
eval `sncfg mget ADMIN_NAME GUEST_NAME ZY_CUSTOM_SHADOW ZY_CUSTOMER`

init_shadow_file()
{
    if [ -n "`echo $ZY_CUSTOMER | grep GP`" ]; then
        #It is GP series
        echo "root:\$1\$38HlpaTA\$bVNplU36JnUr.Xt1IHDCV/:13768:0:99999:7:::" > /tmp/shad
    elif [ -n "`echo $ZY_CUSTOMER | grep HUAWEI`" ]; then
        #It is HUAWEI series
        echo "root:\$1\$7cHnPpHF\$GbYUst3uAh0sFix3fz7B21:13768:0:99999:7:::" > /tmp/shad
    elif [ -n "`echo $ZY_CUSTOMER | grep ZYXEL`" ]; then
        #It is ZYXEL series
        echo "root:\$1\$T6ecjm0M\$EzKDcv0pezh9OItLRG8hY/:13768:0:99999:7:::" > /tmp/shad
    else
        #It is Mitrastar General.
        echo "root:\$1\$CxO9aNna\$nRn0srVBxxmEPQP0H.jeG0:13768:0:99999:7:::" > /tmp/shad
    fi
}

if [ -n "$ADMIN_NAME" ] && [ -n "$GUEST_NAME"  ]; then
    #2011-0304-MattLin
    #Different key account has different password.
    init_shadow_file
    echo "root:x:0:0:,,,:/root:/bin/sh" > /tmp/pass

    #2011-0304-MattLin
    #Add MFG root and password
    echo "mfgroot:\$1\$.3r0/KnH\$eR.mFSJKIiY.y2QsJVsYK.:13768:0:99999:7:::" >> /tmp/shad
    echo "mfgroot:x:0:0:,,,:/root:/bin/sh" >> /tmp/pass
```

OEM customer specific backdoor

Zyxel specific backdoor

OEM customers do not disclose

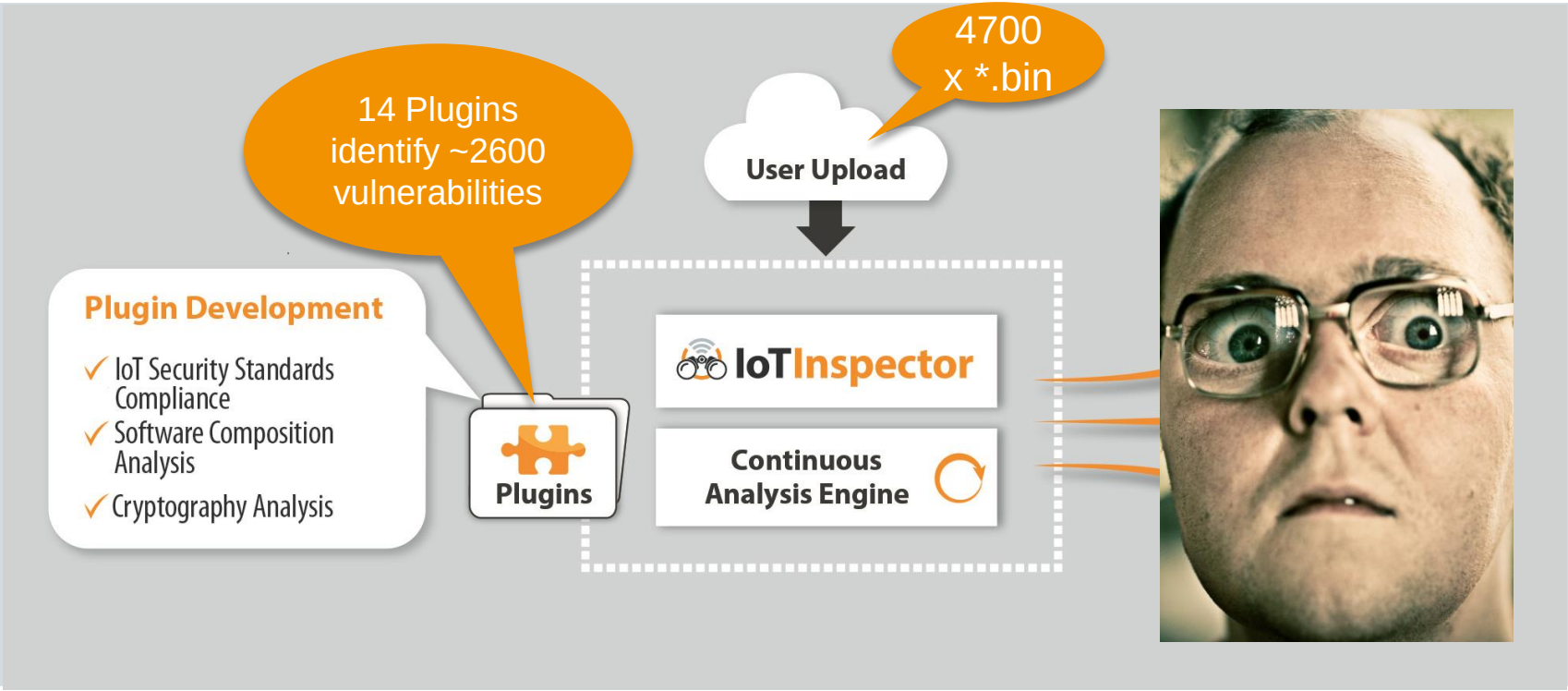
From Huawei PSIRT <PSIRT@huawei.com>
Subject **RE: Do you plan to publish this vulnerability//: Vulnerability in WiMAX Products**
To Me
Cc Huawei PSIRT <PSIRT@huawei.com>, Zhangyan (L) <zhangyan010@huawei.com>

Hi,

Q:Can you share your insights regarding other affected parties (GreenPacket, MADA, ZTE, ZyXEL and MitraStar)?
No. Huawei do not know what is other parties' status.
Q:Who is the OEM/ODM?
Sorry, it is difficult for us to provide this information for this is business information. We will in trouble if we release this information without permission.
Q:Which company is "the source" of the vulnerability?
We really do not know "the source".

what can be **done?**

IoT Inspector – What we are doing?



IoTInspector

www.iot-inspector.com

SEC Consult Vulnerability Lab – IoT Security further readings

https://www.sec-consult.com/vulnerability-lab/index.html
https://www.sec-consult.com/blog/index.html

and what happens
if vendors are waiting to long?

2036

The **FTC has already taken action** against a Taiwanese computer hardware company, requiring a substantial **security program for 20 years.**

Avenue, NW, Washington, D.C. 20580. The reporting period for the Assessments must cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment must:

Source: FTC 23.2.2016, www.ftc.gov

For any further questions contact
your SEC Consult Expert.

Markus Robin

m.robin@sec-consult.com

Tel.: +49 (30) 398 20 2700

SEC Consult Deutschland Unternehmensberatung GmbH
Ullsteinstraße 118, Turm B/8. Stock
12109 Berlin, Deutschland

www.sec-consult.com